REMARKS

The Office Action dated December 18, 2008 has been received and carefully noted. The following remarks are submitted as a full and complete response thereto.

Claims 1-9 and 22-51 are currently pending and are respectfully submitted for consideration. Reconsideration and withdrawal of the rejections is respectfully requested in light of the following remarks.

Claims 50 and 51 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. In particular, the Office Action asserted that the limitation "a computer program, embodied on a computer-readable medium, configured to control a processor" does not appear to be disclosed in the disclosure. However, Applicants respectfully traverse this rejection as follows.

Applicants submit that the Office Action improperly rejected claims 50 and 51 under the first paragraph of 35 U.S.C. § 112, because the Office Action does not set forth express findings of fact which support the lack of written description conclusion. See MPEP § 2163.04(I). According to MPEP § 2163.04(I), the Examiner must:

> (A) Identify the claim limitation(s) at issue; and
>
> (B) Establish a *prima facie* case by providing reasons why a person skilled in the art at the time the application was filed would not have recognized that the inventor was in possession of the invention as claimed in view of the disclosure of the application as filed.

In the instant case, the Office Action has not satisfied element B of the requirement set forth in MPEP § 2163.04(I). In particular, the Office Action merely asserted that the

specification does appear not disclose a computer program, embodied on a computer-readable medium, configured to control a processor, because the Applicant has not pointed out where the new claim is supported. In other words, the Office Action has merely presented an insufficient conclusory statement to improperly reject claims 50 and 51.

Furthermore, the Office Action does not provide reasons why a person skilled in the art would not have recognized that the inventor was in possession of the invention as claimed in view of the disclosure as filed. The Office Action cannot provide such reasons, because the specification clearly states "the preferred embodiment of the present invention is directed to an apparatus, system, method and computer program product that provides network security by verifying the integrity of a remote device requesting access to services that reside on a network" (emphasis added). See specification, page 4, lines 14-16. The specification continues to state "the present invention involves downloading verification software via a network facility, such as an Internet web browser, that can be executed on a remote client device for the purpose of checking or scanning the remote client device to verify that the level of system security is acceptable". See specification, page 4, lines 17-20.

Therefore, in view of the above, a person of ordinary skill in the art would readily appreciate that a "computer program, embodied on a computer-readable medium..." (claims 50 and 51) is supported in specification through implicit disclosure. Applicants

note that MPEP § 2163(I)(B) does **not** require in **haec verba**, but instead **requires** that the limitations added be supported in the specification through express, **implicit**, or inherent disclosure" (emphasis added). Because the MPEP does not require explicit support in the specification, the implicit disclosure of "computer program, embodied on a computer-readable medium" satisfies the written description requirement under the first paragraph of 35 U.S.C. § 112.

Accordingly, Applicants respectfully request that the rejection of claims 50 and 51 be withdrawn for at least the reasons stated above.

Claims 1-9, 22-29, 31, 32, 34-44, 46, and 48-51 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Shaw (U.S. Patent No. 7,058,970) in view of Ji et al. (U.S. Patent No. 6,728,886). Particularly, the Office Action asserted that the combination of Shaw and Ji et al. disclosed all of the elements of claims 1-9, 22-29, 31, 32, 34-44, 46, and 48-51. However, this rejection is respectfully traversed as followed.

Claim 1, upon which claims 2-8 are dependent, recites an apparatus. The apparatus includes a proxy configured to receive a request for network services by at least one remote network device and to perform a security integrity scanning operation on the requesting remote network device. The security scanning operation is performed before and after the remote network device signs on to the proxy. The apparatus includes an authorization processor and access rules controller configured to determine if the remote

network device is authorized to access the requested network services based on the results of the security scanning operation.

Claim 9 recites a system. The system includes at least one remote network device configured to access a network via a network connection to make a request for one or more network resident services. The system includes a gateway configured to receive the request for services and perform a security integrity scanning operation on the remote network device prior to allowing access to the requested network services. The security scanning operation is performed before and after the remote network device signs on to the gateway. The system includes an authentication server configured to verify user authentication credentials of users of remote network that access the network. The system includes at least one network server configured to provide requested network services to at least one remote network accessing the network through the gateway.

Claim 22, upon which claims 23-34 are dependent, recites a method. The method includes performing scanning process and reporting result used in scanning script, comprising at least one variable defined to be used as a vehicle to convey results of a scanning process. The method includes performing at least one scanning operation on the remote network device to verify a security integrity of the remote device. The scanning operation is performed before and after the remote device signs on to a gateway device which is configured to perform the scanning operation. The method includes providing

the results of the scanning operation for purposes of determining whether or not the remote network device is authorized to access the requested network services.

Claim 35, upon which claims 36-48 are dependent, recites a method. The method includes defining at least one access control policy for accessing network services. The access control policy depends, at least in part, on the results of an integrity scan performed on a remote network device. The method includes specifying what scan scripts are to be used under what conditions to the remote network device. The method includes receiving at least one result of an integrity scan from the remote network device at a gateway device. The integrity scan is performed before and after the remote device signs on to the gateway device. The method includes regulating access by the remote network device to network services via the gateway device based, at least in part, on the results of the integrity scan.

Claim 49 recites an apparatus. The apparatus includes a proxying means for receiving a request for network services by at least one remote network device and to perform a security integrity scanning operation on the requesting remote network device. The security scanning operation is performed before and after the remote network device signs on to the proxy. The apparatus includes an authorization processing means and access rules controlling means for determining if the remote network device is authorized to access the requested network services based on the results of the security scanning operation.

Claim 50 recites a computer program, embodied on a computer-readable medium, configured to control a processor to implement a method. The method includes performing scanning process and reporting result used in scanning script, including at least one variable defined to be used as a vehicle to convey results of a scanning process. The method includes performing at least one scanning operation on the remote network device to verify a security integrity of the remote device. The scanning operation is performed before and after the remote device signs on to a gateway device which is configured to perform the scanning operation. The method includes providing the results of the scanning operation for purposes of determining whether or not the remote network.

Claim 51 recites a computer program, embodied on a computer-readable medium, configured to control a processor to implement a method. The method includes defining at least one access control policy for accessing network services. The access control policy depends, at least in part, on the results of an integrity scan performed on a remote network device. The method includes specifying what scan scripts are to be used under what conditions to the remote network device. The method includes receiving at least one result of an integrity scan from the remote network device at a gateway device. The integrity scan is performed before and after the remote device signs on to the gateway device. The method includes regulating access by the remote network device to network services via the gateway device based, at least in part, on the results of the integrity scan.

As will be discussed below, Applicants respectfully submit that the combination of Shaw and Ji et al. fail to disclose, either expressly or implicitly, all of the elements of the claims, and therefore fails to provide the advantages and features discussed above.

Shaw generally discusses an on-connect security scan and delivery by a network security authority. In particular, Shaw discusses a network security authority system that provides on-connect scan and delivery in a virtual lobby to enforce security requirements for a network. See Shaw, Abstract.

Claim 1, however, recites, in part, that "the security scanning operation is performed before and after the remote network device signs on to the proxy" (claim 1, lines 4-5). The Office Action conceded that Shaw does not disclosed the above-quoted feature of claim 1. See Office Action, page 4, lines 5-6. Instead, the Office Action relied upon Ji et al. to disclose the above-quoted feature of claim 1. See Office Action, page 4, lines 6-8.

However, Applicants respectfully submit that Ji et al. does not cure the deficiencies of Shaw, as discussed above with respect to claim 1, for at least the following reasons.

Ji et al. generally discusses distributed virus scanning arrangements and a method thereof. In particular, Ji et al. discusses a method and apparatus to detect viruses that may be transferred between a distributed computer network and a host computer

connected thereto. See Ji et al., column 3, lines 12-14. Stated another way, Ji et al. is merely concerned with scanning for viruses.

This is totally different than "perform[ing] a security integrity scanning operation on the requesting remote network device,...the security scanning operation [being] performed before and after the remote network device signs on to the proxy", as recited in claim 1.

Furthermore, there is no evidence in Ji et al. that there are multiple scanning procedures, i.e., "before and after the remote network device signs on to the proxy", as recited in claim 1. The disclosure of column 3, lines 31-49 of Ji et al. clearly demonstrate a host computer that receives a first set of codes. The first set of codes causes a further download of a second set of codes, which are used to set up a scan. See *Id.* In other words, the system of Ji et al. discusses a two-part process that results in the set up of a scanning procedure. Therefore, it is clear, that the disclosure of Ji et al. does not suggest "perform[ing] a security integrity scanning operation...before and after the remote network device signs on to the proxy", as recited in claim 1.

Moreover, the general discussion provided in column 7 of Ji et al. prevents the disclosure of "the security scanning operation [being] performed before and after the remote network device signs on to the proxy", as recited in claim 1. Column 7, lines 31-43 of Ji et al. states, in part

> [on] the other hand, if the auto-config script detects that the browser is not capable of support local virus scanning...the auto scrip directs that all

> HTTP transfer be performed through a scan engine disposed centrally...in order to allow virus scanning to be performed at the central server. In this manner, all host computers will have virus scanning support and at least a group of host computers will have the virus scanning performed locally in order to relieve the server overload and/or data transfer delay problems encountered in the prior art when the central server is required to perform virus scanning for all host computers.

In other words, Ji et al. discusses a technique that allows virus scan to be performed locally via the host and, if not possible, the virus scan can be performed by a central proxy. However, as noted above, this is different than "perform[ing] a security integrity scanning operation on the requesting remote network device...before and after the remote network device signs on to the proxy", as recited in claim 1.

Therefore, in view of the foregoing, Applicants respectfully submit that Ji et al. fails to cure the deficiencies of Shaw, as discussed above with respect to claim 1. Accordingly, withdrawal of the rejection of claim 1 is respectfully requested.

Claim 9 recites, in part, "wherein the security scanning operation is performed before and after the remote network device signs on to the gateway" (claim 9, lines 6-8). Therefore, Applicants respectfully request that the rejection of claim 9 be withdrawn for reasons similar to those discussed above with respect to claim 1.

Claim 22 recites, in part, "wherein the scanning operation is performed before and after the remote device signs on to a gateway device which is configured to perform the scanning operation" (claim 22, lines 6-8). Therefore, Applicants respectfully request that

the rejection of claim 22 be withdrawn for reasons similar to those discussed above with respect to claim 1.

Claim 35 recites, in part, "wherein the integrity scan is performed before and after the remote device signs on to the gateway device" (claim 35, lines 8-9). Therefore, Applicants respectfully request that the rejection of claim 35 be withdrawn for reasons similar to those discussed above with respect to claim 1.

Claim 49 recites, in part, "wherein the security scanning operation is performed before and after the remote network device signs on to the proxy" (claim 49, lines 4-5). Therefore, Applicants respectfully request that the rejection of claim 49 be withdrawn for reasons similar to those discussed above with respect to claim 1.

Claim 50 recites, in part, "wherein the scanning operation is performed before and after the remote device signs on to a gateway device which is configured to perform the scanning operation" (claim 50, lines 8-10). Therefore, Applicants respectfully request that the rejection of claim 50 be withdrawn for reasons similar to those discussed above with respect to claim 1.

Claim 51 recites, in part, "wherein the integrity scan is performed before and after the remote device signs on to the gateway device" (claim 51, lines 10-11). Therefore, Applicants respectfully request that the rejection of claim 51 be withdrawn for reasons similar to those discussed above with respect to claim 1.

Claims 2-8 depend upon claim 1, claims 23-29, 31, 32, and 34 depend upon claim 22, and claims 36-44 and 48 depend upon claim 35. Therefore, Applicants respectfully request that the rejection of dependent claims 2-8, 23-29, 31, 32, 34, 36-44, and 48 be withdrawn for at least the same and/or similar reasons as their respective base claims, from which they depend upon.

Claims 30, 33, 45, and 47 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Shaw in view of Ji et al., and further in view of Hiltgen (U.S. Patent Publication No. 2003/0177392). Particularly, the Office Action asserted that the combination of Shaw, Ji et al. and Hiltgen disclosed all of the elements of claims 30, 33, 45, and 47. However, this rejection is respectfully traversed as followed.

Shaw and Ji et al. are discussed above. Hiltgen generally discusses a secure user authentication over a communication network. In particular, Hiltgen discusses performing user authentication over a client in communication via a first network with a a server infrastructure including an application server. See Hiltgen, paragraph [0012].

However, Applicants respectfully submit that Hiltgen does not cure the deficiencies of Shaw and Ji et al., as discussed above with respect to claims 22 and 35. For example, Hiltgen does not disclose, either expressly or implicitly, at least, "wherein the scanning operation is performed before and after the remote device signs on to a gateway device which is configured to perform the scanning operation", as recited in claim 22, and as similarly recited in claim 35.

Claims 30 and 33 are dependent upon claim 22 and claims 45 and 47 are dependent upon claim 35. Therefore, Applicants respectfully request that the rejection of dependent claims 30, 33, 45, and 47 be withdrawn for at least the same and/or similar reasons as their respective base claims, from which they depend upon.

For at least the reasons discussed above, Applicants respectfully submit that none of the cited references, whether considered alone or in combination, disclose, either expressly, implicitly or inherently, all of the elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1-9 and 22-51 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Sheetal S. Patel
Attorney for Applicants
Registration No. 59,326

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY L.L.P.
14th Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

SSP:dk